IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Immonen

Title: SECURE SESSION SET UP
                 BASED ON THE WIRELESS
                 APPLICATION PROTOCOL

Appl. No.:   09/720,971

International   7/3/1999
Filing Date:
371(c) Date: 1/3/2001

Examiner: Zachary A. Davis

Art Unit: 2137

Confirmation   8278
Number:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the New **Pre-Appeal Brief Conference Pilot Program**, announced July 11, 2005, this Pre-Appeal Brief Request is being filed together with a Notice of Appeal.

REMARKS

In the May 15, 2007 Office Action, the Examiner objected to paragraph [0009] and maintained his rejection of claims 1-12, 15-40, and 42-68 under 35 U.S.C. §103(a) as being unpatentable over PCT Publication WO97/24831 (Ichikawa), E.U. Patent Publication EP 0538216 (Anvret et al.), US Patent No. 6,240,512 (Fang et al.), and/or US Patent No. 5,845,519 (Weiss). Applicant traverses the above for the reasons set forth below.

As to paragraph [0009], a comma merely differentiates between one described advantage and an exemplary situation when that advantage is realized by a user. Therefore, Applicant submits that the Examiner's objection is unwarranted.

Regarding Ichikawa, the Examiner asserted that Ichikawa teaches all of the required limitations of claim 1[1], except for the use of public and private keys. As described in Applicant's previously filed response of March 7, 2007, which is incorporated herein by reference in its entirety, Ichikawa merely teaches a system and method of generating data encryption keys in conjunction with a smartcard, e.g., a smartcard which Ichikawa describes as "the device" or "the client" and a smartcard reading/processing unit or server, such as an ATM machine. (*See, e.g.,* Abstract, page 4, lines 6-7, page 6, lines 9-10, page 10, lines 14-20, and pages 13-14). Despite the Examiner's assertions on pages 2-3 of the outstanding Office Action that the ATM scenario focused on in the Detailed Description of Ichikawa is merely an example, the generic allusion to wireless applications made in the Background of is insufficient to teach the limitations in various claims of the present application relating to algorithm selection for data communications, wireless connection requests, wireless messaging, etc. Because Ichikawa characterized the smartcard as a device or client 102 that communicates with a server 502, Applicant submits that it is impossible for Ichikawa to be interpreted as teaching the required limitations of claim 1, for example, let alone a wireless communication apparatus, a data communication apparatus, and separate unit.

Moreover, notwithstanding the above, as described in Applicant's previously filed response, Ichikawa fails to teach many of the required limitations of, e.g., claim 1 of the present application. For example, at page 3 of the outstanding Office Action, the Examiner asserted that his "interpretation" of Ichikawa's selected series number (SSN) is that which "actually provides the information regarding the selected algorithm (i.e. the variation of the series number is equivalent to variation of the algorithm used in generating.)" Applicant disagrees. Ichikawa is clear at page 7, lines 4-8 that "[a] selection algorithm 114 that is

---

[1] As noted in Applicant's previously filed response, although claim 1 is discussed, Applicant's arguments contained herein apply to other independent claims as applicable. Moreover, the Examiner copied, word for word, his previous rejection without addressing Applicant's further contention that the Examiner's "blanket" rejection of claims 5, 15, 19. 22-24, and 46 was improper because these claims contain certain other limitations and/or features not recited in independent claim 1.

executed by the smartcard 102 is used to select the SSN 116." Moreover, page 4, lines 9-12, page 8, lines 3-4, page 11, lines 12-16 of Ichikawa indicate that a SSN is merely an input to an encryption algorithm. The Examiner's indication that varying series numbers equates to varying an algorithm is a fabrication that is without any support in Ichikawa. That is, stored bit combinations, SSNs, can be used by a single, not chosen algorithm, DEA1, for encryption purposes, but regardless there is no selection of algorithms taught by Ichikawa.

Applicant further submits that Ichikawa fails to teach a wireless communication apparatus that generates a master secret code and calculates a signature based in part, on the chosen algorithm. As described previously, a derived key (DK) cannot read on the claimed master secret code of the present application. Moreover, although the Examiner asserted at pages 3-4 of the outstanding Office Action that Applicant misunderstood his reasoning and/or presented confusing arguments, Applicant merely rebutted the Examiner's own reasoning. At pages 9-10 of the outstanding Office Action (copied from the previous Office Action), the Examiner stated that "the wireless apparatus generating a master secret code (page 4, lines 10-12) and calculating a signature based on the chosen algorithm and the master secret code (page 4, lines 12-15)." Page 4, lines 10-12 of Ichikawa indicate that "[t]he selected SN is then encrypted by a conventional data encryption algorithm using the MK to generate a Derived Key (DK)." Because claim 1 requires "generation" of a master secret code, Applicant assumed that the DK was interpreted as the claimed master secret code and described in the previous response why Ichikawa in light of this teaching does not read on, e.g., claim 1. Now, the Examiner has indicated that Ichikawa's MK reads on the claimed master secret code. Applicant submits that even this interpretation fails because Ichikawa's MK is stored on a smartcard along with several SNs, and is therefore not generated, as required by claim 1, for example. (*See, e.g.,* page 4, lines 5-12 and page 6, lines 16-18).

In response to the Examiner's assertions regarding Applicant's alleged attacking of singular references, Applicant submits that it was the Examiner who indicated and maintains that the only limitation of claim 1 not taught by Ichikawa is the use of public and private keys. Accordingly, on pages 16-20 of Applicant's previously filed response, Applicant focused on every limitation except for the use of public and private keys when rebutting the Examiner's position that all of the limitations of claim 1 except for the use of public and

private keys could be found in Ichikawa. To wit, the only mention of public and private keys made in pages 16-20 was on pages 17 and 20, where Applicant provided a brief overview/summary of the claims and recited limitations.

As to Anvret et al., the Examiner maintained his rejection and asserted in response to Applicant's previously filed response, that private keys are associated with an algorithm for generating a signature. Applicant disagrees. In particular, Applicant submits that the Examiner has used a piecemeal approach to combining references that happen to use like terms, but has failed to provide sound reasoning as to why Anvret et al. combined with Ichikawa read on the claims of the present application. As noted in Applicant's previously filed response at page 21, "although Anvret et al. discusses the use of public keys, private keys as described in the <u>context</u> of claim 1 are not taught." (emphasis added). Applicant further described in detail that the exchange of identities, public keys, and signature in Anvret et al. <u>occurs upon initial contact</u>. (*See, e.g.,* page 21 of Applicant's previously filed response of March 27, 2007).[2] In contrast, claim 1, for example, requires that the exchanging of at least the public key is performed after the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection. Moreover, the signature is neither generated nor exchanged until after messaging has occurred between the wireless and data communication apparatuses. The use of a private key in this context is not taught or even suggested by Anvret et al. Therefore, Anvret et al. does not cure the already-discussed deficiencies of Ichikawa.

With regard to Fang et al., the Examiner has maintained his previous rejection and further asserted at page 6 of the outstanding Office Action that because master keys are distributed in response to some initiation, the "initiation must include some sort of message indicating distribution of the keys is to take place." Applicant submits that notwithstanding the Examiner's overreaching comment that "some sort of message" is inherent, the fact remains that claim 1, for example, requires that the message is comprised of a public key and information about which algorithm the data communication apparatus has chosen, where the

---

[2] Applicant notes that the Examiner is in violation of Section 707.07(f) of the MPEP at least with respect to Anvret et al. because the Examiner maintained his rejection, but failed to answer the substance of Applicant's arguments.

message is transmitted from the data communication apparatus back to a wireless communication apparatus. Certainly, "some sort of message indicating distribution of the keys is to take place" falls well short of the required limitations recited above with regard to the claimed message. Moreover, as to Applicant's further attempted rebuttal of Applicant's arguments with regard to Fang et al., Applicant submits that such arguments are moot in light of the Examiner's characterization of "a message" as taught by Fang et al. However, Applicant maintains that the Examiner continues to mischaracterize and misinterpret the teachings of each of the above-discussed references in an attempt to arrive at the claims recited in the present application. Therefore, Applicant repeats by incorporation those arguments presented in Applicant's response filed March 7, 2007.

As to Weiss, Applicant previously presented detailed arguments as to why Weiss does not cure the deficiencies of Ichikawa, Anvret et al., and Fang et al. In response, the Examiner merely stated that it does. Applicant submits that such a statement does not amount to a proper rebuttal or substantive answer to Applicant's arguments. Moreover, Applicant submits that a "period" of time within which storage occurs suggests a beginning and an end, whereas "permanent" storage suggest that there is no end to the time of storage. Therefore, combining Weiss with any of the prior cited references would not be obvious or at the least would result in an inoperable system/method.

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance.

Respectfully submitted,

Date: <u>September 17, 2007</u>   By   /G. Peter Albert Jr./

FOLEY & LARDNER LLP   G. Peter Albert Jr.
Customer Number: 30542   Attorney for Applicant
Telephone: (858) 847-6735   Registration No. 37,268
Facsimile: (858) 792-6773

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 061602-1525

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] On September 17, 2007 Signature Typed or printed name	Application Number 09/720,971	Filed 7/3/1999
	First Named Inventor Olli Immonen	
	Art Unit 2137	Examiner Zachary A. Davis

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number   37,268

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34

/G. Peter Albert Jr./
Signature

G. Peter Albert Jr.
Typed or Printed Name

(858) 847-6735
Telephone Number

September 17, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒   *Total of 1 forms are submitted.

DLMR_324577.1